

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

24. 6. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 3 年 7 月 2 5 日

出 願 番 号  
Application Number: 特 願 2 0 0 3 - 2 7 9 6 3 7  
[ST. 10/C]: [ J P 2 0 0 3 - 2 7 9 6 3 7 ]

出 願 人  
Applicant(s): 沖電気工業株式会社

REC'D 19 AUG 2004

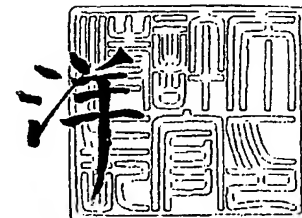
WIPO PCT

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2 0 0 4 年 8 月 6 日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川



【書類名】 特許願  
【整理番号】 SA003816  
【あて先】 特許庁長官殿  
【国際特許分類】 G06K 9/36  
【発明者】  
    【住所又は居所】 東京都港区虎ノ門 1 丁目 7 番 1 2 号 沖電気工業株式会社内  
    【氏名】 井戸田 誠一  
【特許出願人】  
    【識別番号】 000000295  
    【氏名又は名称】 沖電気工業株式会社  
【代理人】  
    【識別番号】 100082050  
    【弁理士】  
    【氏名又は名称】 佐藤 幸男  
【手数料の表示】  
    【予納台帳番号】 058104  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 9100477

**【書類名】 特許請求の範囲****【請求項 1】**

認証対象の身体上の特徴を用いて生体認証し、当該生体認証の結果が肯定的であるときに、その後、当該肯定的な生体認証の結果を前提とした簡易かつ迅速な認証を行える認証媒体を発行する過程と、

前記認証媒体を用いて認証対象を認証し、当該認証媒体による認証の結果に応じて機器の使用を許可する過程とから成ることを特徴とする生体認証併用複合認証方法。

**【請求項 2】**

前記認証媒体は、認証対象である機器使用者の所有物であることを特徴とする請求項 1 記載の生体認証併用複合認証方法。

**【請求項 3】**

前記認証媒体は、パスワードであることを特徴とする請求項 1 記載の生体認証併用複合認証方法。

**【請求項 4】**

前記認証媒体である所有物を回収する過程を伴うことを特徴とする請求項 2 記載の生体認証併用複合認証方法。

**【請求項 5】**

認証対象の身体上の特徴を用いて生体認証する生体認証部と、当該生体認証の結果が肯定的であるときに、認証媒体を発行する媒体発行部とから成る第 1 の認証装置と、

前記認証媒体を用いて認証対象を認証する媒体認証部と、当該認証媒体による認証の結果に応じて機器の使用を許可する機器制御部から成る第 2 の認証装置を備えたことを特徴とする生体認証併用複合認証システム。

**【請求項 6】**

前記認証媒体は、認証対象である機器使用者の所有物であることを特徴とする請求項 5 記載の生体認証併用複合認証システム。

**【請求項 7】**

前記認証媒体は、パスワードであることを特徴とする請求項 5 記載の生体認証併用複合認証システム。

**【請求項 8】**

前記認証媒体である所有物を回収する回収部を備えたことを特徴とする請求項 6 記載の生体認証併用複合認証システム。

**【請求項 9】**

前記第 1 の認証装置は機器使用者の所有物にその後の認証に必要なすべてのデータを書き込み、

前記第 2 の認証装置は前記所有物から取得したデータのみをもとに単独で機器使用を許可するか否かを判定し得ることを特徴とする請求項 6 記載の生体認証併用複合認証システム。

**【請求項 10】**

前記認証媒体である所有物を回収する過程において生体認証を伴うことを特徴とする請求項 4 記載の生体認証併用複合認証方法。

**【請求項 11】**

前記認証媒体である所有物を回収する回収部を備えた認識装置内に、当該所有物の回収時に生体認証する生体認証部を備えたことを特徴とする請求項 8 記載の生体認証併用複合認証システム。

## 【書類名】明細書

## 【発明の名称】生体認証併用複合認証方法及びシステム

## 【技術分野】

## 【0001】

本発明は、ICカードや磁気カード等の所有物による個人認証やパスワードによる認証と、バイオメトリクス認証を複合した認証方法及びシステムに関するものである。

## 【背景技術】

## 【0002】

個人認証の方式として従来以下のものがある。

- (1) 1つは、所有物による個人認証方式である。これは、ICカードや磁気カードを個人が所有し、そのカードにあらかじめ個人のIDや情報を格納しておくことにより個人認証する方式である。
- (2) もう1つは、バイオメトリクスを利用した個人認証方式である。これは、指紋や虹彩等の個人の身体的特徴を用いる認証方式である。

## 【発明の開示】

## 【発明が解決しようとする課題】

## 【0003】

図23において、上述の各認証方式の特徴を比較して示す。図示のように「所有物による個人認証」と「バイオメトリクス個人認証」とは対称的な特徴を示す。

すなわち、「所有物による個人認証」は低費用で認識でき、認証時間が高速であるメリットがある。その反面、悪用される危険性があるとともに、所有物を携帯していないときは認証できないなどのデメリットを有している。

## 【0004】

一方、「バイオメトリクス認証」は悪用される危険性が低く、個人の身体特徴のため確実に認証可能であるメリットをもつ。その反面、認証装置が高価となり、認証時間に比較的時間を要するデメリットを有する。

## 【課題を解決するための手段】

## 【0005】

そこで、本発明は以上の点を解決するため、「所有物による個人認証」と「バイオメトリクス個人認証」を複合することでそれぞれのメリット、デメリットを補うシステムを構成する。

すなわち、次の構成を採用する。

## 【0006】

## 〈構成1〉

1つは、生体認証併用複合認証方法であり、認証対象の身体上の特徴を用いて生体認証し、当該生体認証の結果が肯定的であるときに、その後、当該肯定的な生体認証の結果を前提とした簡易かつ迅速な認証を行える認証媒体を発行する過程と、前記認証媒体を用いて認証対象を認証し、当該認証媒体による認証の結果に応じて機器の使用を許可する過程とから成ることを特徴とする。

これは、1度、安全確実な生体認証を行った後は、簡易かつ迅速な認証を行うようにしたものである。

## 【0007】

この方法は、例えば、認証対象の身体上の特徴を用いて生体認証する生体認証部と、当該生体認証の結果が肯定的であるときに、認証媒体を発行する媒体発行部とから成る第1の認証装置と、前記認証媒体を用いて認証対象を認証する媒体認証部と、当該認証媒体による認証の結果に応じて機器の使用を許可する機器制御部から成る第2の認証装置を備えた生体認証併用複合認証システムにおいて使用される。

## 【0008】

## 〈構成2〉

もう1つは、構成1のシステムにおいて、第1の認証装置は機器使用者の所有物にその

後の認証に必要なすべてのデータを書き込み、第2の認証装置は前記所有物から取得したデータのみをもとに単独で機器使用を許可するか否かを判定し得ることを特徴とする。

これは、第1の認証装置と、第2の認証装置とを通信回線で接続できない状況でも、構成1の方法を使用できるシステムである。

【0009】

〈構成3〉

さらにもう1つは、構成1の方法において、認証媒体である所有物を回収する過程で生体認証を伴うことを特徴とする。

あるいは、構成1または構成2のシステムにおいて、認証媒体である所有物を回収する回収部を備えた認識装置内に、当該所有物の回収時に生体認証する生体認証部を備えたことを特徴とする。

これらは、生体認証を活用して、所有物が機器使用者にとって不要となった後に、その所有物を他の者に利用させることができないような保証を作ろうとするものである。

【発明を実施するための最良の形態】

【0010】

以下、本発明の最良の実施の形態を実施例を用いて説明する。

【実施例1】

【0011】

図1は、本発明の実施例1のシステム構成図である。図1において、管理装置11は本システム全体を管理し、所有物あるいはパスワードによる認証と、バイオメトリクス認証を複合した認証を行う。この管理装置11は、認証装置A12、認証装置B13、認証装置C14とネットワークで接続されている。

認証装置A12は、バイオメトリクス認証装置12-1と、カード発行装置12-2と、制御機器12-3と、結果表示装置12-4を備えている。

【0012】

制御機器12-3の例として、電気錠や課金装置があげられる。なお、図示の例では、カード発行装置12-2とともに、制御機器12-3を備えるようにしたが、制御機器を備えない構成でもよい。

結果表示装置12-4は、LEDやLCDを使い使用者に結果を通知する装置である。

使用者は認証装置A12を使い、バイオメトリクス認証を行う。そして、カードを受け取る。この際、図示のような構成のものでは、同時に、ドアの開錠や金銭の支払いをすることができる。

【0013】

認証装置B13は、カードリーダー13-1と、制御機器13-2と、結果表示装置13-3を備えている。

制御機器13-2の例として、電気錠や課金装置があげられる。

使用者は認証装置B13においてカードを使いドアの開錠や支払いをすることができる。

【0014】

認証装置C14は、カード回収装置14-1と、制御機器14-2と、結果表示装置14-3を備えている。

カード回収装置14-1は、カードリーダーの機能を備えてもよい。

【0015】

制御機器14-2の例として、電気錠や課金装置があげられる。なお、図示の例では、制御機器14-2を備えたが、制御機器は備えない構成でもよい。

使用者はカード回収装置14-1にてカードを返却する。この際、図示の構成のものでは、同時に、ドアの開錠や金銭の支払いをすることができる。

【0016】

図2から図5までは、図1の各機器の機能ブロック図である。

図2は、管理装置11の機能ブロック図である。図2において、認証データ受信部101は、認証装置A12からの認証データを受信する。

## 【0017】

図6に認証データの一例を示す。認証データは登録者DB109のIDとリンクしているユニークな番号である「ID」、認証装置A12を識別するための「装置ID」等の情報から構成される。

図2に戻り、登録者DB検索部102は、IDをキーにして登録者DB109からデータを検索する。

## 【0018】

図7に登録者DB109の例を示す。登録者DB109はユニークな番号である「ID」、「名前」、カードを発行済みか否かを判定する「カード発行状態」、カードを使用可能な有効期限を示す「カード有効期限」、使用権限のある装置を示す「使用権限」等の情報により構成される。

## 【0019】

図2に戻り、カード発行判定部103は、認証データのIDで検索された登録者DB109の「カード発行状態」、「使用権限」等からカード発行するか否かを判定する。カード発行判定の一例としては「カード発行状態」が未発行であり、認証装置A12の使用権限が「使用可」である場合カードを発行可と判定する手法があげられる。

## 【0020】

カード発行判定結果送信部104は、カード発行判定の結果およびカード入力データを認証装置A12に送信する。

図8にカード入力データの一例を示す。カード入力データは登録者DB109のIDとリンクしているユニークな番号である「ID」等の情報により構成される。

## 【0021】

図2に戻り、登録者DB更新部105は、登録者DB109の「カードの発行状況」と「カード有効期限」等を更新する。

装置データ受信部106は、認証装置B13または認証装置C14から装置データを受信する。

## 【0022】

図9に装置データを示す。装置データは登録者DB109のIDとリンクしているユニークな番号である「ID」、装置を識別するために装置毎に固有に与えられた「装置ID」等の情報により構成される。

## 【0023】

図2に戻り、装置使用判定部107は、装置データのIDから検索された登録者DB109の「カード有効期限」および「使用権限」等より、装置の使用を許可するか否かを判定する。装置使用判定の一例としてはカードの有効期限内であり、使用権限が使用可になっている場合があげられる。

## 【0024】

装置使用判定結果送信部108は、装置使用判定部107での判定結果を認証装置B13または認証装置C14に送信する。

## 【0025】

図3は、認証装置A12の機能ブロック図である。図3において、バイOMETRICS認証部121は、図1のバイOMETRICS認証装置12-1を用いて使用者のバイOMETRICSデータを取得する。そして、これを、あらかじめバイOMETRICSDB128に登録されているバイOMETRICSデータとマッチングすることにより使用者を認証する。

## 【0026】

図7にバイOMETRICSDB128の一例を示す。バイOMETRICSDBは登録者DB109のIDとリンクしているユニークな番号の「ID」と個人を認証するためのデータである「バイOMETRICSデータ」等の情報から構成されている。図3に示す例では、バイOMETRICSDBを認証装置A12に設けたが、管理装置11に設けてネットワークを介して管理装置11においてバイOMETRICS認証を実施してもよい。

## 【0027】

結果表示部122は、バイオメトリクス認証の結果やカード発行判定結果等を結果表示装置12-4により使用者に通知する。

【0028】

認証データ送信部123は、認証データを管理装置11へ送信する。認証データはバイオメトリクスDB128から取得した「ID」と認証装置A12の装置ID等からなる（図6参照）。

カード発行判定結果受信部124は、管理装置11から送信されたカード発行判定結果を受信する。

【0029】

カード発行部125は、カード入力データを書込み、カードをカード発行装置12-2から発行する。

制御部126は、制御機器12-3を制御する。たとえば制御機器12-3が電子錠の場合は電子錠を開錠する。なお、ここでは制御機器12-3を制御するものとしたが、制御機器12-3が備えられていない構成ではカードの発行を実施後、制御機器の制御はしない。

【0030】

図4は、認証装置B13の機能ブロック図である。図4において、カードデータ読取り部131は、図1のカードリーダ13-1を用いてカード入力データを読込む。

装置データ送信部132は、装置データを管理装置11へ送信する。装置データはカード入力データおよび装置IDからなる（図9）。

【0031】

装置使用判定結果受信部133は、図1の管理装置11から装置使用判定結果を受信する。

結果表示部134は、装置使用判定を図1の結果表示装置13-3に表示する。

【0032】

制御部135は、装置使用判定がOKの場合、図1の制御機器13-2を制御する。たとえば、制御機器13-2が電子錠の場合は電子錠を開錠する。

【0033】

図5は、認証装置C14の機能ブロック図である。図5において、カードデータ読取り部141は、カード機能を持ったカード回収装置14-1を用いてカード入力データを読込む。

装置データ送信部142は、装置データを管理装置11へ送信する。

【0034】

装置使用判定結果受信部143は、管理装置11から装置使用判定結果を受信する。

結果表示部144は、装置使用判定を結果表示装置14-4に表示する。

カード回収部145は、カード回収装置14-1を用いてカードを回収する。

【0035】

制御部146は、装置使用判定がOKの場合、制御機器14-2を制御する。たとえば、制御機器14-2が電子錠の場合は電子錠を開錠する。なお、ここではカードのデータにより制御機器を制御しているが、カード回収のみを実施し制御機器の制御は実施しない形態でもよい。また、制御機器を制御するに際しては、カードのデータにより制御機器を制御せずに、カード回収をトリガにして制御機器を制御する手法もある。

【0036】

〈実施例1の動作〉

図11、12、13における実施例1の動作のフローチャートに沿って、本実施例の動作を説明する。

図11は、認証装置A12での認証動作を示す。

まず、S101で、バイオメトリクス認証部121はバイオメトリクス認証を実施する。そして、認証ができた場合はS103の処理へ移る。認証ができない場合はS102の処理へ移る。

【0037】

S102で、結果表示部122は使用者に認証ができなかったことを通知する。

S103で、認証データ送信部123は認証データを管理装置11に送信する。

【0038】

ここで、管理装置の動作が始まる。

まず、S 104で、認証データ受信部101は認証データを受信する。

そして、S 105で、登録者DB検索部102は受信した認証データのIDをもとに登録者DB 109上のデータを検索する。

【0 0 3 9】

S 106で、カード発行判定部103は検索したデータよりカード発行するか否かを判定する。

また、S 107で、登録者DB更新部105は登録者DB 109のデータを更新する。

【0 0 4 0】

S 108で、カード発行判定結果送信部104は認証装置A 12へ結果を送信する。カード発行可の場合はカード発行可の結果とカード入力データを送信する。また、カード発行不可の場合はカード発行不可の結果を送信する。

【0 0 4 1】

ここで、認識装置Aの動作が再開される。

S 109で、カード発行判定結果受信部124はカード発行判定結果を受信する。

S 110で、結果表示部122はカード発行判定結果を使用者に通知する。

S 111で、カード発行部125はカード発行可の場合、S 112の処理へ移る。カード発行不可の場合は終了する。

【0 0 4 2】

S 112で、カード発行部125はカード入力データを書込んだカードを発行する。

S 113で、制御部126は所定の動作を実施する。たとえば認証装置Aに電気錠が設けられているならば電気錠の開錠を実施する。

【0 0 4 3】

図 1 2 は、認証装置B 13での認証動作を示す。

まず、S 121で、カードデータ読取り部131は認証装置A 12で発行されたカードのカード入力データを読取る。

S 122で、装置データ送信部132は装置データを管理装置11へ送信する。

【0 0 4 4】

ここで、管理装置の動作が始まる。

S 123で、装置データ受信部106は装置データを受信する。

S 124で、登録者DB検索部102は受信した認証データのIDをもとに登録者DB 109上のデータを検索する。

S 125で、装置使用判定部107は検索したデータから認証装置B 13の使用許可するか否かを判定する。

S 126で、装置使用判定結果送信部108は認証装置B 13へ結果を送信する。

【0 0 4 5】

ここで、認証装置Bの動作が再開される。

S 127で、装置使用判定結果受信部133は結果を受信する。

S 128で、結果表示部134は装置使用判定結果を使用者に通知する。

S 129で、制御部135は装置使用可の場合は処理をS 130へ移す。使用不可の場合は処理を終了する。

S 130で、制御部135は所定の動作を実施する。たとえば、認証装置B 13に電気錠が設けられているならば電気錠の開錠を実施する。

【0 0 4 6】

図 1 3 は、認証装置C 14での認証動作を示す。

まず、S 141で、カードデータ読取り部141は認証装置A 12で発行されたカードのカード入力データを読取る。

S 142で、装置データ送信部142は装置データを管理装置11へ送信する。

【0 0 4 7】

ここで、管理装置の動作が始まる。

S143で、装置データ受信部106は装置データを受信する。

S144で、登録者DB検索部102は受信した認証データのIDをもとに登録者DB109上のデータを検索する。

S145で、装置使用判定部107は検索したデータから認証装置C14の使用許可するか否かを判定する。

S146で、装置使用判定結果送信部108は認証装置C14へ結果を送信する。

#### 【0048】

ここで、認証装置Cの動作が再開される。

S147で、装置使用判定結果受信部143は結果を受信する。

S148で、結果表示部144は装置使用判定結果を使用者に通知する。

S149で、カード回収部145は装置使用可の場合は処理をS151へ移す。使用不可の場合はS150へ処理を移す。

#### 【0049】

S150で、カード回収部145はカードを使用者に返却する。これにより、処理終了する。

S151で、カード回収部145はカードを回収する。

S152で、制御部135は所定の動作を実施する。たとえば、認証装置C14に電気錠が設けられているならば電気錠の開錠を実施する。

#### 【0050】

なお、上述した実施例においては、カード等の所有物による認証とバイオメトリクス認証を複合させるものについて説明したが、本発明はこれに限らず、暗証すなわちパスワードによる認証とバイオメトリクス認証を複合させたものによっても同様に実現できるものである。この点、後述する実施例についても同様である。

#### 【0051】

##### 〈実施例1の効果〉

以上詳述したように、実施例1のシステムによりバイオメトリクス認証と所有物による認証の両方の利便性を得ることが可能となる。すなわち、本システムによりバイオメトリクス認証による安全性および随時携帯しなくてよいという利便性を得るとともに、所有物による認証による即座に認証可能であるという利便性を得ることが可能となる。

#### 【0052】

例えば、会社等の施設での運用を考える。会社の門では認証装置A12でバイオメトリクス認証を実施し、カードを取得する。ここでは、バイオメトリクス認証を実施するため高い安全性を確保できる。この際、カードはこの場で発行されるため、カードを携帯する必要はない。会社内ではこのカードと認証装置B13を使う。このカードで食堂での支払いや、入退室管理を実施する。バイオメトリクスでは照合に時間がかかるケースがあるため食堂等で混雑する可能性があるが、カードは即座に認証可能なため混雑することはない。このカードは最後会社から退社する際に認証装置C14で回収する。従って会社の外にカードがもちだされることはないため盗難等の危険性は低い。

#### 【0053】

また、本システムをマンションの管理システムに応用した場合には、マンションの入口で本システムに登録された住民は認証装置A12によりバイオメトリクス認証を受け、カードあるいはキーを取得する。ここで、バイオメトリクス認証の実施により高度のセキュリティを確保できる。この際、カードやキーはこの場で発行されるため、それらを携帯して外出する必要はない。自宅に入るときはこのカードあるいはキーと認証装置B13を使う。このカードやキーは外出する際にマンションの出口に設けられた認証装置C14で回収する。従ってマンションの外にこれらがもちだされることはないため盗難等の危険性は低くなる。

#### 【実施例2】

#### 【0054】

図14は、実施例2のシステム構成図である。実施例1と異なる点は管理装置11と認証装置A12はネットワークで接続されているが、認証装置B13と認証装置C14は管理装置11

に接続されていない点である。その他の構成は実施例 1 と同様である。

#### 【0055】

図 15 および 16 は、各機器の機能ブロック図である。管理装置と認証装置 A の機能ブロック図は、実施例 1 と同様である。図 17 は、実施例 2 でのカード入力データの一例である。カード入力データはユニークな番号である「ID」、カードを使用可能な有効期限を示す「カード有効期限」、使用権限のある装置を示す「使用権限」等の情報により構成される。

#### 【0056】

図 15 は、認証装置 B13 の機能ブロック図である。図 15 において、カードデータ読取り部 231 は、カードリーダ 13-1 を用いてカード入力データを読込む。装置使用判定部 232 は、「カード有効期限」、「使用権限」等より装置の使用を許可するか否かを判定する。装置使用判定の一例としてはカード有効期限内であり、装置毎に割り当てられている「装置 ID」の使用権限が使用可の場合、使用を許可する手法があげられる。

#### 【0057】

結果表示部 233 は、装置使用判定部 232 における結果を結果表示装置 13-3 に表示する。制御部 234 は、装置使用判定が OK の場合、制御機器 13-2 を制御する。たとえば、制御機器 13-3 が電子錠の場合は電子錠を開錠する。

#### 【0058】

図 16 は、認証装置 C14 の機能ブロック図である。図 16 において、カードデータ読取り部 241 は、カード機能を持ったカード回収装置 14-3 を用いてカード入力データを読込む。装置使用判定部 242 は、「カード有効期限」、「使用権限」等より装置の使用を許可するか否かを判定する。

#### 【0059】

結果表示部 243 は、装置使用判定を結果表示装置 14-4 に表示する。カード回収部 244 は、カード回収装置 14-1 を用いてカードを回収する。制御部 245 は、装置使用判定が OK の場合、制御機器 14-3 を制御する。たとえば、制御機器 14-3 が電子錠の場合は電子錠を開錠する。

#### 【0060】

##### 〈実施例 2 の動作〉

図 18 および 19 の実施例 2 の動作のフローチャートに沿って、本実施例の動作を説明する。

実施例 1 における図 11 の S101～S113 までの動作は実施例 2 も同じように行われるものである。ただし、カード入力データが図 17 の内容になる。

#### 【0061】

図 18 は、認証装置 B13 での認証動作である。

まず、S221 で、カードデータ読取り部 231 は認証装置 A12 で発行されたカードのカード入力データを読取る。

S222 で、装置使用判定部 232 はカード入力データから認証装置 B13 の使用許可するか否かを判定する。

そして、S223 で、結果表示部 233 は装置使用判定結果を使用者に通知する。

#### 【0062】

S224 で、制御部 234 は装置使用可の場合は処理を S225 へ移す。使用不可の場合は処理を終了する。

S225 で、制御部 234 は所定の動作を実施する。たとえば、認証装置 B13 に電気錠が設けられているならば電気錠の開錠を実施する。

#### 【0063】

図 19 は、認証装置 C14 での認証動作を示す。

まず、S241 で、カードデータ読取り部 241 は認証装置 A12 で発行されたカードのカード入力データを読取る。

S242 で、装置使用判定部 242 はカード入力データから認証装置 C14 を使用許可するか否

かを判定する。

そして、S243で、結果表示部243は装置使用判定結果を使用者に通知する。

【0064】

S244で、カード回収部244は装置使用可の場合は処理をS246へ移す。使用不可の場合はS245へ処理を移す。

S245で、カード回収部244はカードを使用者に返却する。これで、処理を終了する。

S246で、カード回収部244はカードを回収する。

【0065】

S247で、制御部245は所定の動作を実施する。たとえば、認証装置C14に電気錠が設けられているならば電気錠の開錠を実施する。

【0066】

〈実施例2の効果〉

以上詳述したように、実施例2によれば、実施例1と異なり、以下の効果がある。すなわち、実施例1では認証装置B13と認証装置C14がネットワークに接続されている必要があったが、実施例2では、これらの装置はネットワークとは接続されていない。このため、これらの装置をネットワークにつなげることができないような環境でも、実施例1と同様の効果を得られる。

【0067】

例えばコンドミニアムの運用を考える。コンドミニウムがある場所はネットワーク環境が整備されていないような場所とする。使用者は認証装置A11を使いカードを取得する。認証装置A11はネットワーク接続可能な場所に設置されている。このカードを認証装置B13が設置されているコンドミニウムで使用することでコンドミニウムの錠を開錠でき、設備の使用が可能となる。

【実施例3】

【0068】

図20は実施例3のシステム構成図である。実施例1と異なる点は認証装置C14にバイオメトリクス認証装置が備えられたことである。管理装置11と認証装置A12と認証装置B13は実施例1と同様である。

【0069】

認証装置C34は、バイオメトリクス認証装置34-1と、カード回収装置34-2と、制御機器34-3と、結果表示装置34-4を備えている。ここでは、実施例1の構成に認証装置C34を備えたが、実施例2の構成に認証装置C34を備えてもよい。

【0070】

図21は各機器の機能ブロック図である。管理装置11と認証装置A12と認証装置B13は実施例1の機能ブロック図と同様である。

そこで、図21では認証装置C34の機能ブロックのみを示す。図21において、バイオメトリクス認証部341は、バイオメトリクス認証装置34-1を用いて使用者のバイオメトリクスデータを取得し、あらかじめバイオメトリクスDB349に登録されているバイオメトリクスデータとマッチングすることにより使用者を認証する。

【0071】

カードデータ読取り部342は、カードリーダ機能を持ったカード回収装置34-2を用いてカード入力データを読込む。カード所有者判定部343は、カード内のIDとバイオメトリクス認証で取得できたIDが一致するか否かを判定する。装置データ送信部344は、装置データを管理装置11へ送信する。装置使用判定結果受信部345は、管理装置11から装置使用判定結果を受信する。

【0072】

結果表示部346は、装置使用判定を結果表示装置34-4に表示する。カード回収部347は、カード回収装置34-2を用いてカードを回収する。制御部348は、装置使用判定がOKの場合、制御機器34-3を制御する。たとえば、制御機器34-3が電子錠の場合は電子錠を開錠する。ここではカードのデータにより制御機器を制御しているが、カード回収をトリガにし

て制御機器を制御する手法や、カード回収のみを実施し、制御機器の制御は実施しない形態でもよい。

#### 【0073】

〈実施例3の動作〉

実施例1における図11のS101～S113、図12のS121～S130までの動作は実施例3でも同じである。

#### 【0074】

図22は認証装置C34での認証動作を示す。

まず、S341で、バイオメトリクス認証部341はバイオメトリクス認証を実施する。認証ができた場合はS343の処理へ移る。認証ができない場合はS342の処理へ移る。

S342で、結果表示部346は認証結果NGを使用者に通知する。そして、ここで処理を終了する。

#### 【0075】

一方、S343で、結果表示部346は認証結果OKを使用者に通知する。

S344で、カードデータ読取り部342は認証装置A12で発行されたカードのカード入力データを読取る。

S345で、カード所有者判定部343はバイオメトリクス認証で得られたIDとカード入力データのIDが一致するか否かを判定する。そして、一致する場合はS347の処理へ移行する。一致しない場合はS346の処理へ移行する。

#### 【0076】

S346で、結果表示部346はIDが一致しないことを使用者に通知する。

S347で、装置データ送信部344は装置データを管理装置11へ送信する。これにより、管理装置での処理が始められる。

#### 【0077】

S348で、装置データ受信部106は装置データを受信する。

S349で、登録者DB検索部102は受信した認証データのIDをもとに登録者DB109上のデータを検索する。

S350で、装置使用判定部107は検索したデータから認証装置C34の使用許可するか否かを判定する。

S351で、装置使用判定結果送信部108は認証装置C34へ結果を送信する。これにより、認証装置Cの動作が再開される。

#### 【0078】

S352で、装置使用判定結果受信部345は結果を受信する。

S353で、結果表示部346は装置使用判定結果を使用者に通知する。

S354で、カード回収部347は装置使用可の場合は処理をS356へ移す。使用不可の場合はS355へ処理を移す。

S355で、カード回収部347はカードを使用者に返却する。これで処理を終了する。

#### 【0079】

S356では、カード回収部347はカードを回収する。

S357で、制御部348は所定の動作を実施する。たとえば、認証装置Aに電気錠が設けられているならば電気錠の開錠を実施する。

#### 【0080】

〈実施例3の効果〉

実施例3によりある人がバイオメトリクス認証を実施して取得したカードを第三者が取得して不正利用することを防止することができる。

#### 【0081】

例としてスキー場のリフト券を考える。スキー場ではリフト券の転売問題が存在する。ある人が購入したリフト券を第三者に転売することで同じリフト券で2名以上が使用する問題である。認証装置C34を使用することでそのリフト券が購入者のものか否かを判定できるため転売問題のような不正利用を防止できる。

## 【0082】

具体的には、リフト券の購入時に認証装置Aでその購入者から保証金を預かり、認証装置Cでリフト券の返還を条件としてバイオメトリクス認証で確認したその購入者にその保証金を返すようにする。

## 【図面の簡単な説明】

## 【0083】

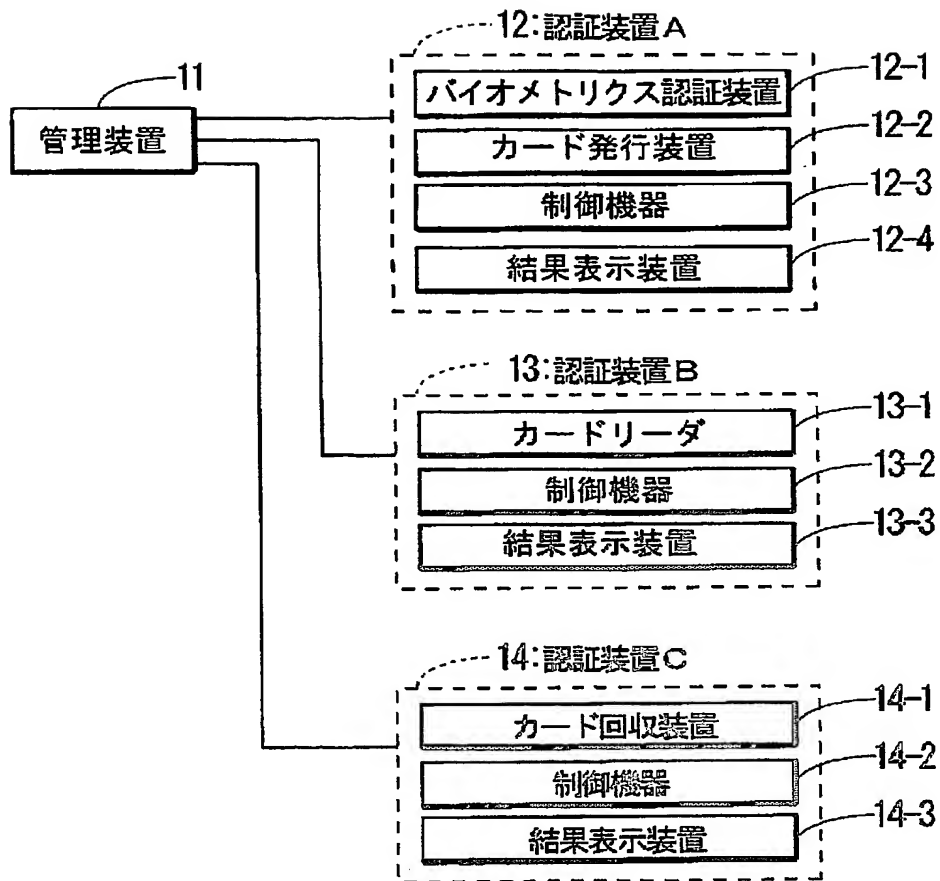
- 【図1】 本発明の実施例1のシステム構成を示すブロック図である。
- 【図2】 図1の管理装置の機能構成を示すブロック図である。
- 【図3】 図1の認証装置Aの機能構成を示すブロック図である。
- 【図4】 図1の認証装置Bの機能構成を示すブロック図である。
- 【図5】 図1の認証装置Cの機能構成を示すブロック図である。
- 【図6】 認証データの一例を示す図である。
- 【図7】 登録者DBの一例を示す図である。
- 【図8】 カード入力データの一例を示す図である。
- 【図9】 装置データの一例を示す図である。
- 【図10】 バイオメトリクスデータの一例を示す図である。
- 【図11】 認証装置Aでの認証動作を示すフローチャートである。
- 【図12】 認証装置Bでの認証動作を示すフローチャートである。
- 【図13】 認証装置Cでの認証動作を示すフローチャートである。
- 【図14】 本発明の実施例2のシステム構成を示すブロック図である。
- 【図15】 図14の認証装置Bの機能構成を示すブロック図である。
- 【図16】 図14の認証装置Cの機能構成を示すブロック図である。
- 【図17】 実施例2でのカード入力データの一例を示す図である。
- 【図18】 実施例2の認証装置Bでの認証動作を示すフローチャートである。
- 【図19】 実施例2の認証装置Cでの認証動作を示すフローチャートである。
- 【図20】 本発明の実施例3のシステム構成を示すブロック図である。
- 【図21】 図20の認証装置Cの機能構成を示すブロック図である。
- 【図22】 実施例3の認証装置Cでの認証動作を示すフローチャートである。
- 【図23】 所有物による認証とバイオメトリクス認証との比較内容の説明図である。

## 【符号の説明】

## 【0084】

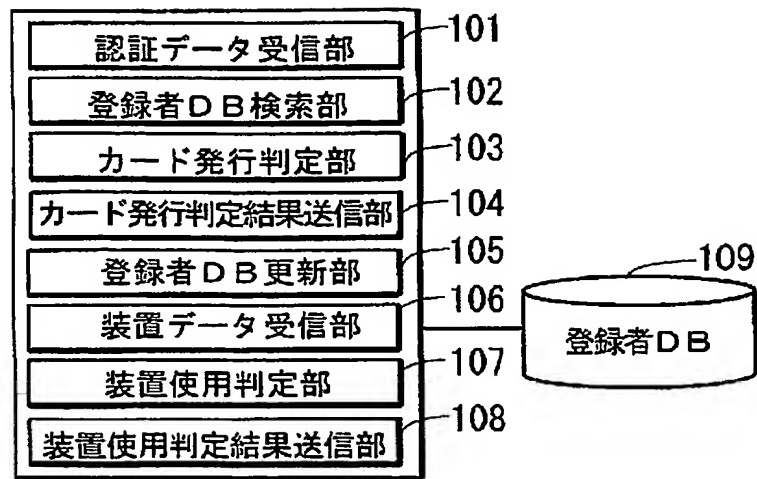
- 11 管理装置
- 12 認証装置A
- 13 認証装置B
- 14 認証装置C

【書類名】 図面  
【図 1】



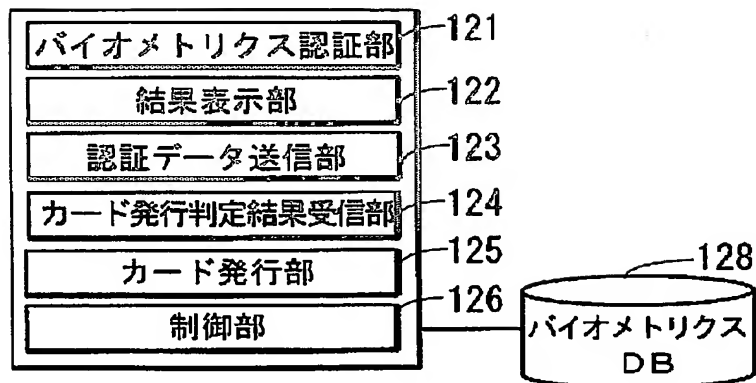
本発明の実施例 1 のシステム

【図 2】



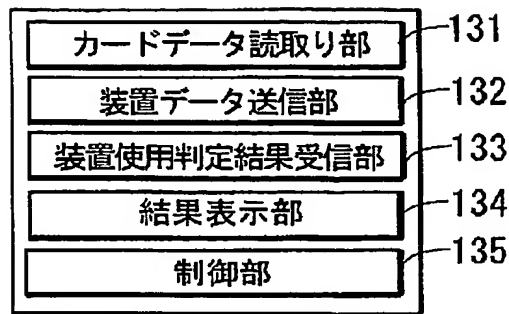
管理装置の機能構成

【図 3】



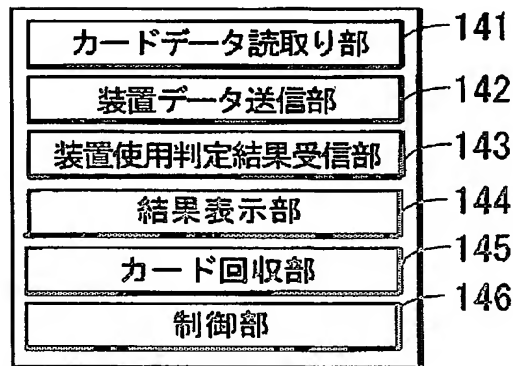
認証装置Aの機能構成

【図 4】



認証装置 B の機能構成

【図 5】



認証装置 C の機能構成

【図 6】

I D	装置 I D
X X X X X X	A A A A A A
X X X X X X	A A A A A A
.	

認証データの一例

【図 7】

ID	名前	カード 発行状態	カード 有効期限	使用権限		
				装置 ID1	装置 ID2	.
XXXXXX	沖 太郎	未発行	——	使用可	使用可	.
XXXXXX	山田 次郎	発行	hh:mm:ss	使用不可	使用可	.
.	.	.	.	.	.	.

登録者 DB の一例

【図 8】

I D
X X X X X X
X X X X X X
.

カード入力データの一例

【図 9】

I D	装置 I D
X X X X X X	A A A A A A
X X X X X X	A A A A A A
.	.

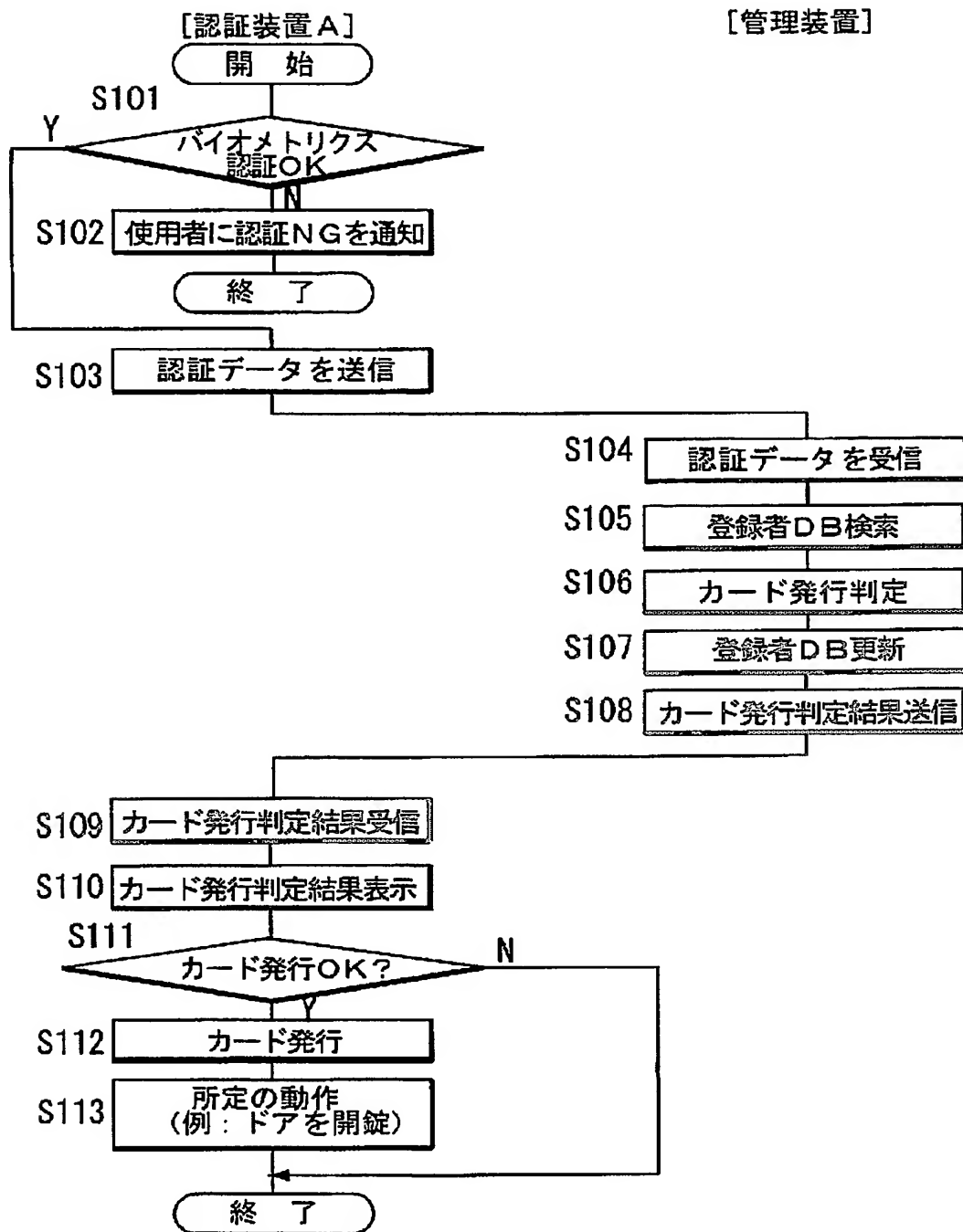
装置データの一例

【図 1 0】

I D	バイオメトリクスデータ
X X X X X X	* * * * * * * * *
X X X X X X	* * * * * * * * *
.	.

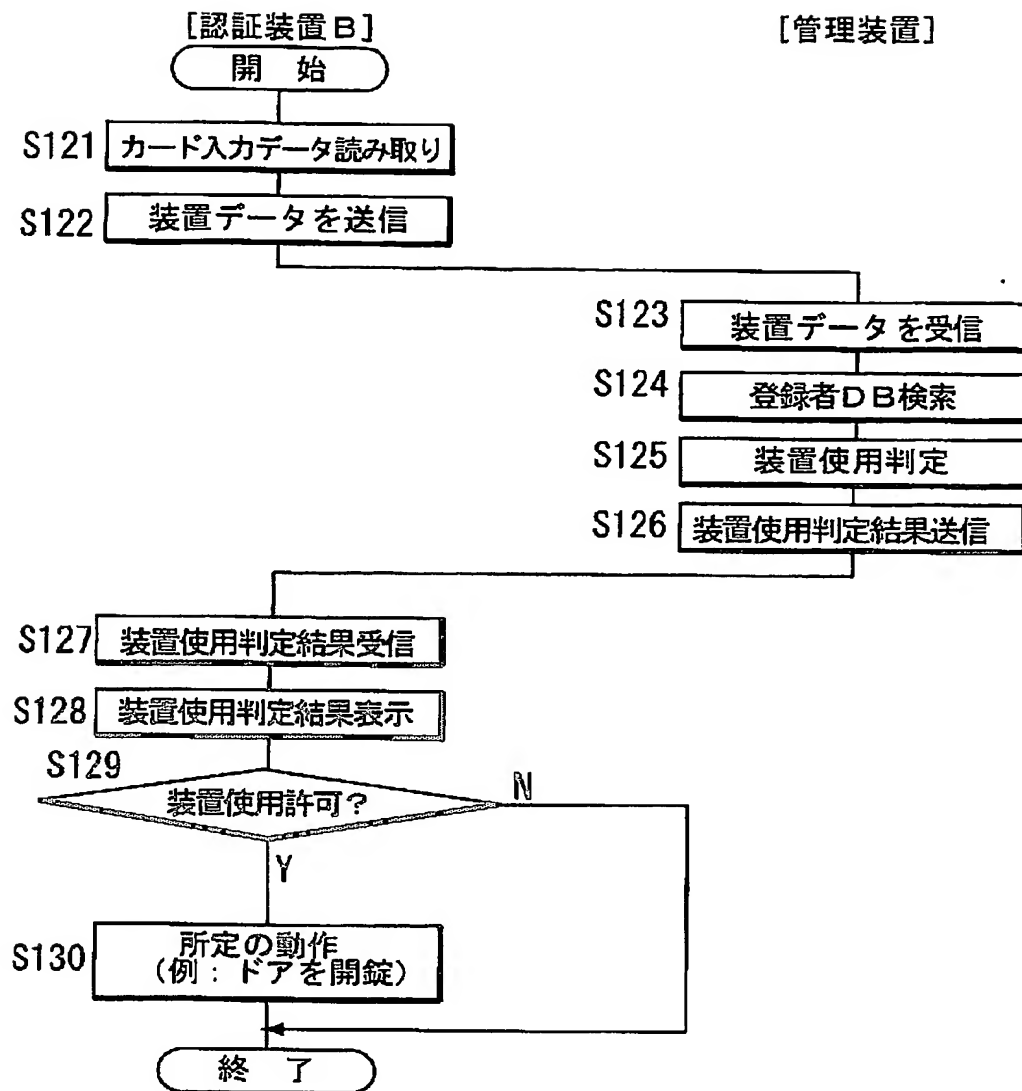
バイオメトリクスデータの一例

【図 11】



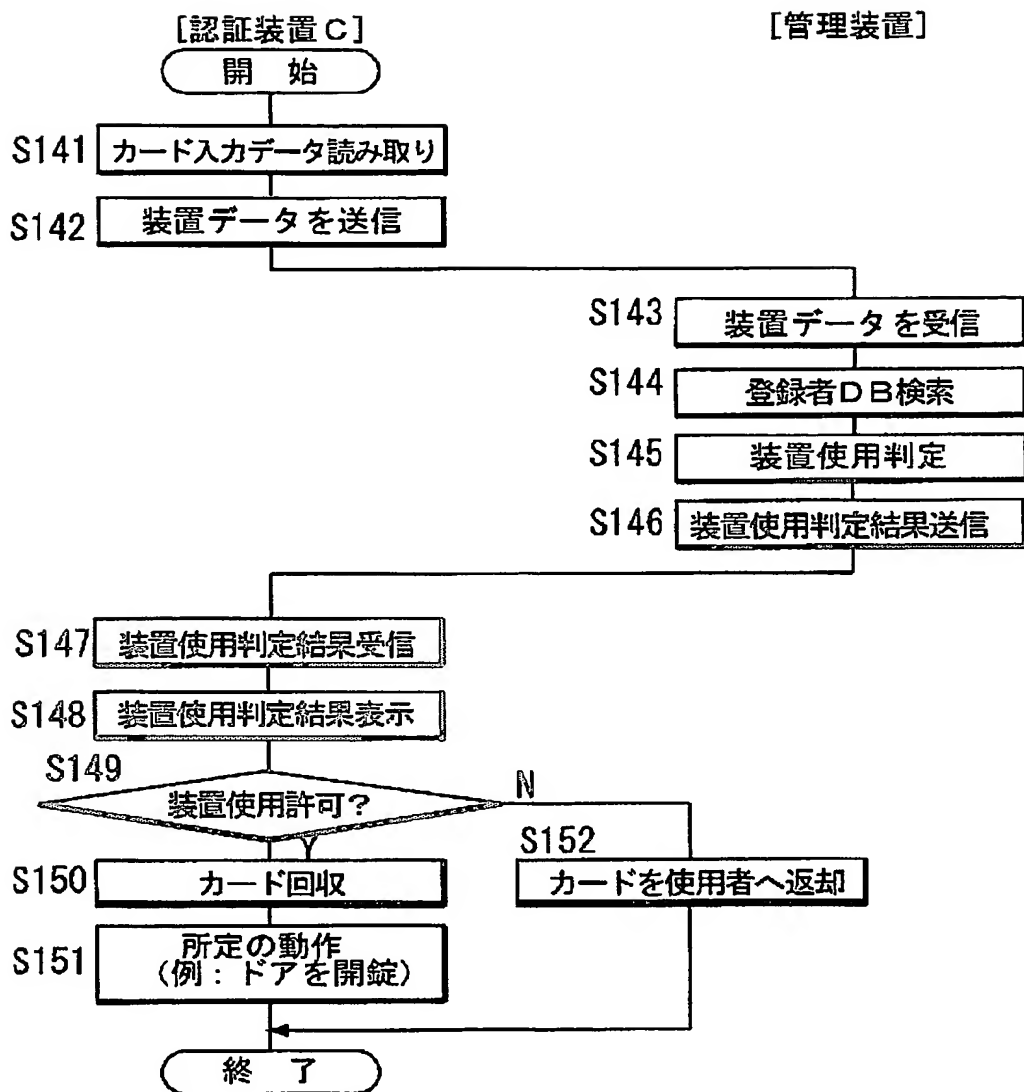
実施例 1 の認証装置 A での認証動作

【図 12】



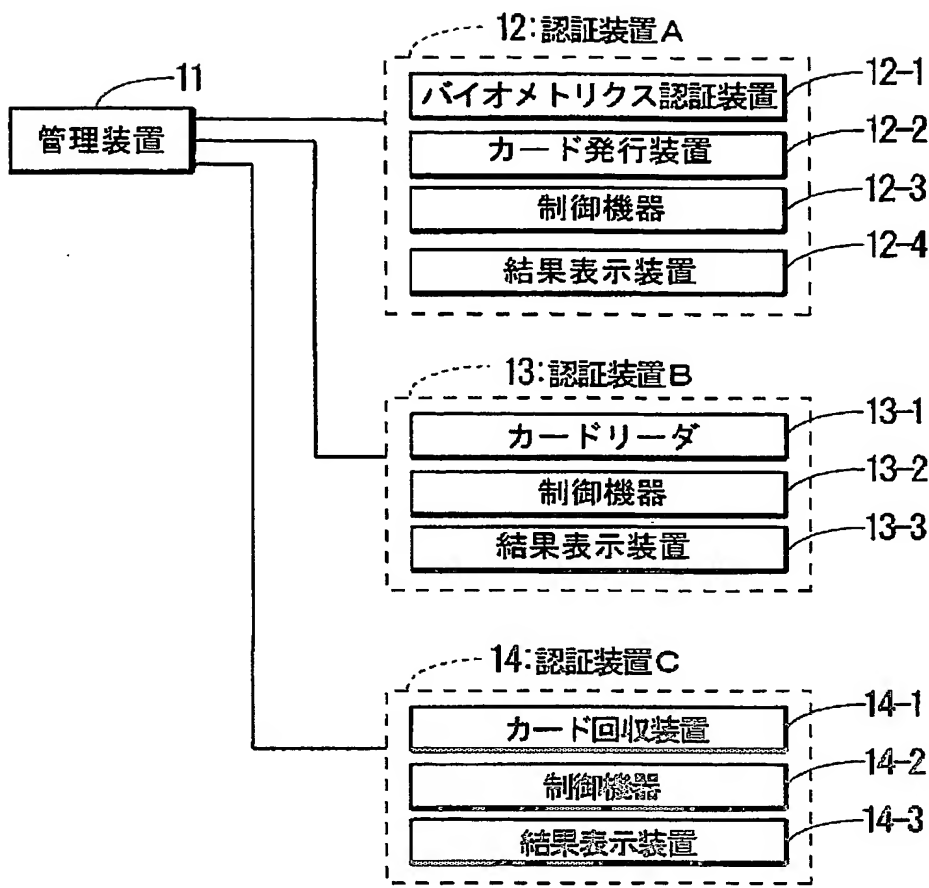
実施例 1 の認証装置 B での認証動作

【図 13】



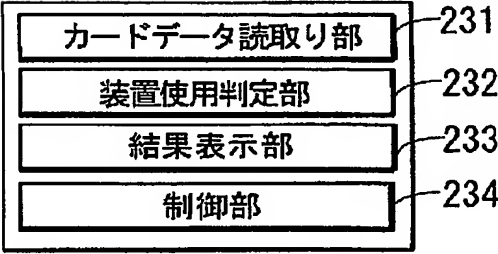
実施例 1 の認証装置 C での認証動作

【図 1 4】



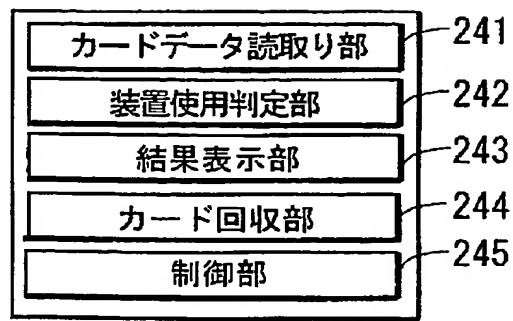
本発明の実施例 2 のシステム

【図 1 5】



認証装置 B の機能構成

【図 16】



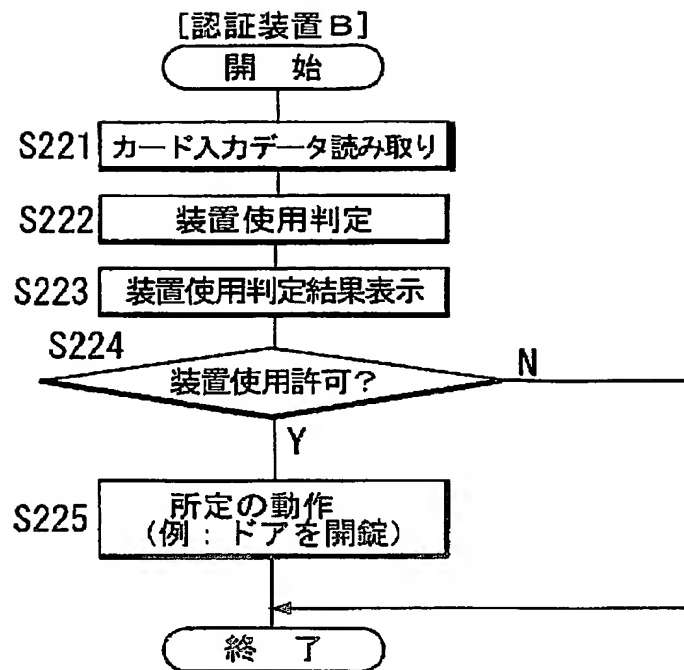
認証装置Cの機能構成

【図 17】

ID	カード 有効期限	使用権限		
		装置ID1	装置ID2	・
XXXXXX	———	使用可	使用可	・
XXXXXX	hh:mm:ss	使用不可	使用可	・
・	・	・	・	・

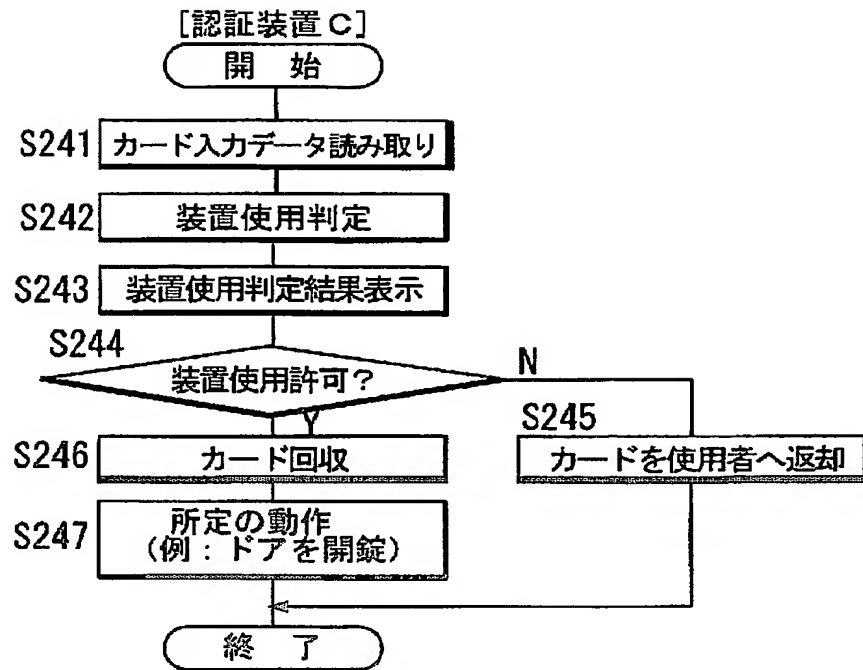
カード入力データの一例

【図 18】



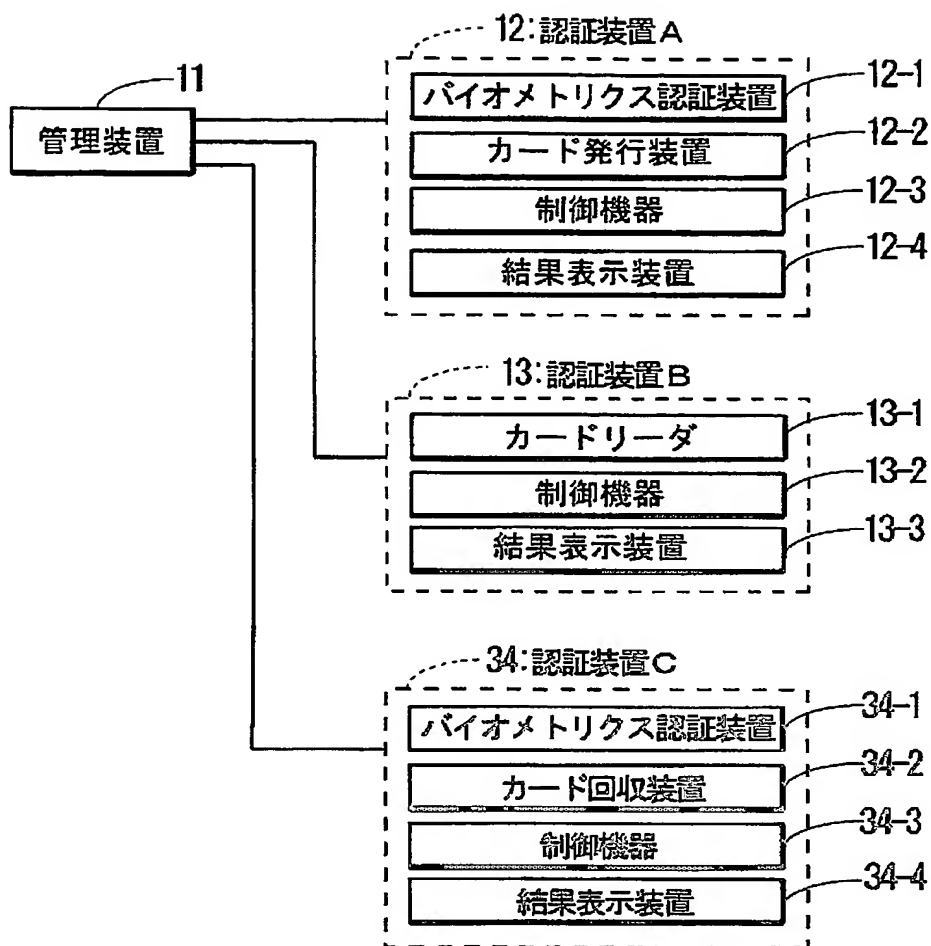
実施例 2 の認証装置 B での認証動作

【図 19】



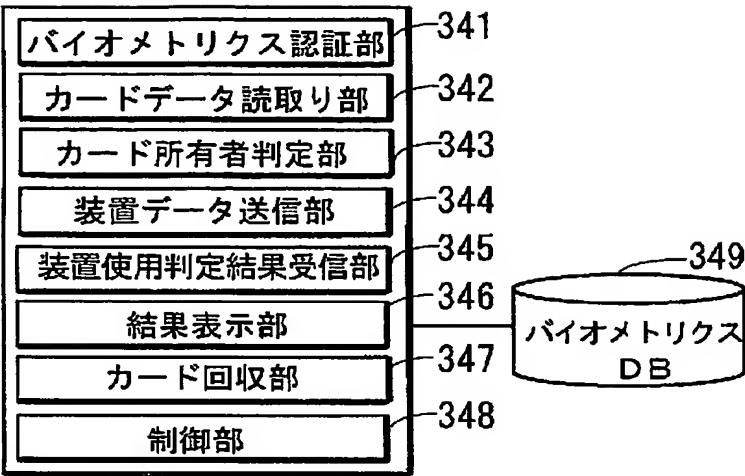
実施例 2 の認証装置 C での認証動作

【図 20】



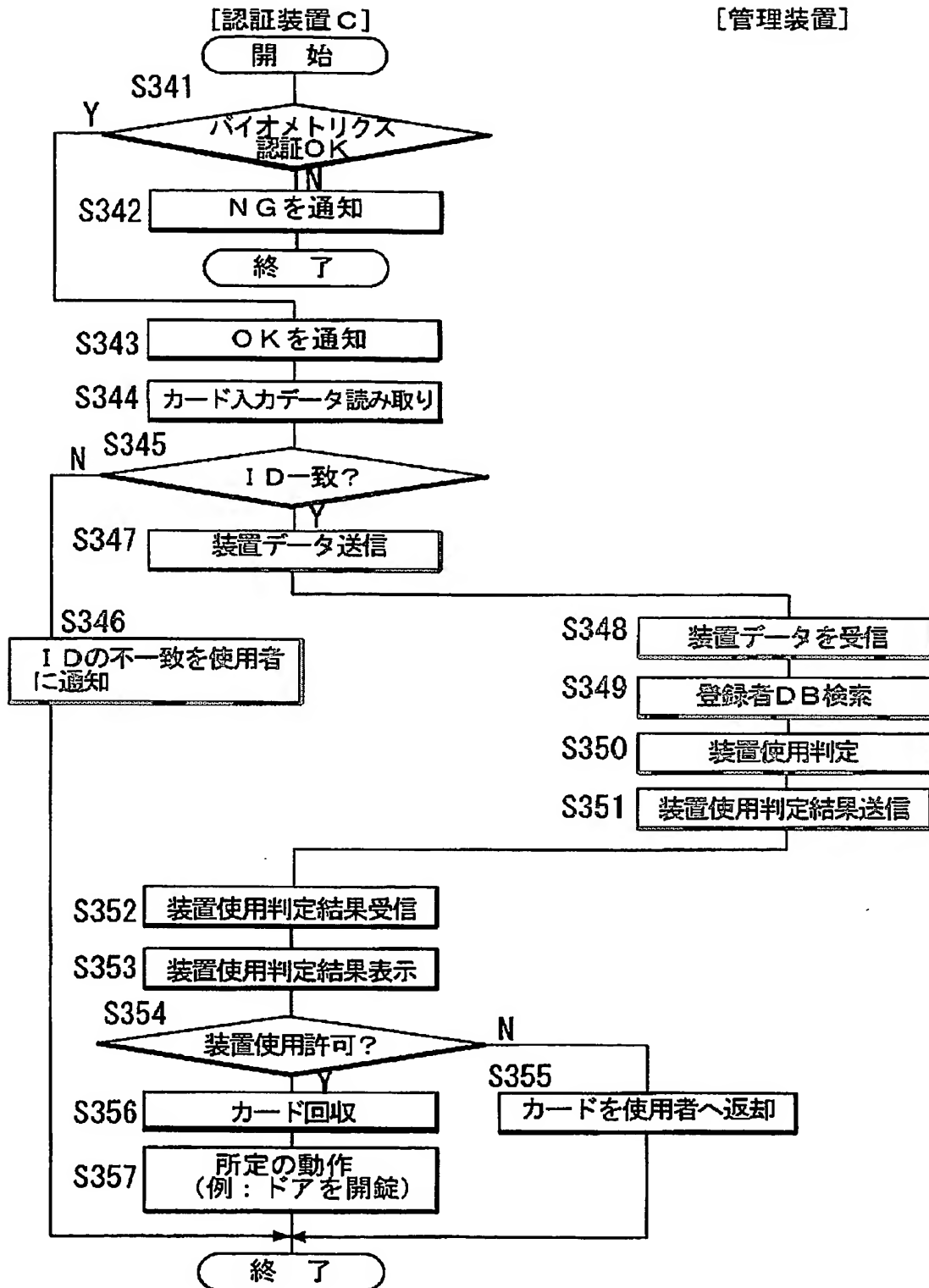
本発明の実施例 3 のシステム

【図 2 1】



実施例 3 の認証装置 C の機能構成

【図 22】



実施例 3 の認証装置 C での認証動作

【図 23】

	所有物		バイオメトリクス
	磁気カード、ICカードなど	指紋、虹彩、顔貌など	
費用の安さ	○	×	・所有物による個人認証に比べ高価
悪用の困難さ	×	◎	・偽造は困難
認証時間の速さ	○	△	・認証に時間を要するケースがある
確実な認証	△	◎	・身体特徴のため確実に認証可能

所有物による認証とバイオメトリクス認証との比較

【書類名】要約書

【要約】

【課題】生体認証と通常の認証との双方の利点を引き出す。

【解決手段】生体認証併用複合認証システムは、少なくとも、第 1 の認証装置 A 1 2 と、第 2 の認証装置 B 1 3 とを備え、これらを管理する管理装置 1 1 を備える。第 1 の認証装置 A 1 2 は、認証対象である機器使用者の身体上の特徴を用いて生体認証するバイオメトリクス認証装置 12-1 と、当該生体認証の結果が肯定的であるときに、認証媒体であるカードを発行するカード発行装置 12-2 とを含む。第 2 の認証装置 B 1 3 は、前記カードを用いて使用者を認証するために当該カードを読み取るカードリーダー 13-1 と、当該カードによる認証の結果に応じて機器の使用を許可する制御機器 13-2 とを含む。これらの装置を各方式の認証の特性に応じて使い分ける。なお、カードは、認証装置 C 1 4 に設けられたカード回収装置 14-1 で回収するようにしても良い。

【選択図】図 1

認定・付加情報

特許出願の番号	特願 2003-279637
受付番号	50301228963
書類名	特許願
担当官	第七担当上席 0096
作成日	平成15年 7月28日

<認定情報・付加情報>

【提出日】 平成15年 7月25日

特願 2 0 0 3 - 2 7 9 6 3 7

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 0 2 9 5 ]

1. 変更年月日 1 9 9 0 年 8 月 2 2 日

[変更理由] 新規登録

住 所 東京都港区虎ノ門 1 丁目 7 番 1 2 号

氏 名 沖電気工業株式会社